

(18 U.S.C. App.), and the “Security Procedures Established Pursuant to Public Law 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information,” and other applicable authorities.

Subpart B—Classified Information

§ 7.20 Classification and declassification authority.

(a) Top Secret original classification authority may only be exercised by the Secretary and by officials with a demonstrable and continuing need to exercise such authority and to whom such authority is delegated in writing by the Secretary. The Chief Security Officer, as the Senior Agency Official, is delegated authority to originally classify information up to and including Top Secret. No official who is delegated Top Secret original classification authority by the Secretary may further delegate such authority.

(b) The Chief Security Officer may delegate Secret and Confidential original classification authority to other officials with a demonstrable and continuing need to exercise such authority. No official who is delegated original classification authority by the Secretary or the Chief Security Officer may further delegate such authority.

(c) Persons who are delegated original classification authority shall attend mandatory classification training within 60 days of the delegation, and annually thereafter. Persons who fail to attend mandatory training shall have such authority suspended until such time as the training occurs.

(1) Except for suspensions of the Inspector General’s classification authority, the Chief Security Officer may waive a suspension of authority for no longer than 60 days following the due date of the training when unavoidable circumstances exist that prevent the person from attending the training.

(2) For cases involving suspension of the Inspector General’s classification authority under paragraph (c) of this section, only the Secretary or Deputy Secretary may waive such a suspension.

(d) Officials authorized to classify information at a specified level are also authorized to classify information at a

lower level. In the absence of an official authorized to exercise classification authority, the person designated to act in lieu of such official may exercise the official’s classification authority.

(e) Declassification authority may be exercised by the official who authorized the original classification, if that official is still serving in the same position and has original classification authority; the originator’s current successor in function, if that individual has original classification authority; a supervisory official of either the originator or his or her successor in function, if the supervisory official has original classification authority; or officials delegated declassification authority by the Secretary or the Chief Security Officer.

§ 7.21 Classification of information, limitations.

(a) Information may be originally classified only if all of the following standards are met:

(1) An original classification authority is classifying the information;

(2) The information is owned by, produced by or for, or is under the control of the United States Government;

(3) The information falls within one or more of the categories of information specified in section 1.4 of Executive Order 13526; and

(4) The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to cause identifiable and describable damage to the national security.

(b) Information shall be classified as Top Secret, Secret, or Confidential in accordance with and in compliance with the standards and criteria in Executive Order 13526. No other terms shall be used to identify United States classified information except as otherwise provided by statute.

(c) If there is significant doubt about the need to classify information it shall not be classified. If classification is warranted but there is significant doubt about the appropriate level of classification it shall be classified at the lower level.

(d) Original classification decisions made by a DHS original classification

§ 7.22

6 CFR Ch. I (1–1–15 Edition)

authority shall be incorporated into a security classification guide in a timely manner but no later than one year from the date of the original decision. Such decisions shall be reported to the Office of the Chief Security Officer, Administrative Security Division, within thirty days following the original classification decision.

(e) All DHS security classification guides shall be coordinated through and receive the concurrence of the Office of the Chief Security Officer, Administrative Security Division, prior to approval and publication by an original classification authority.

(f) Information shall not be classified in order to:

- (1) Conceal inefficiency, violations of law, or administrative error;
- (2) Prevent embarrassment to a person, organization, or agency;
- (3) Restrain competition;
- (4) Prevent or delay release of information that does not require protection in the interest of national security.

(g) Information may not be reclassified after it has been declassified and released to the public under proper authority unless:

(1) The reclassification is approved in writing by the Secretary based on a document-by-document determination that the reclassification of the information is required to prevent significant and demonstrable damage to the national security;

(2) The reclassification of the information meets the standards and criteria for classification pursuant to Executive Order 13526;

(3) The information may be reasonably recovered without bringing undue attention to the information; and

(4) The reclassification action is reported promptly to the Assistant to the President for National Security Affairs (National Security Advisor) and the Director of ISOO.

(5) For documents in the physical and legal custody of the National Archives and Records Administration that have previously been made available for public use and determined to warrant reclassification per paragraphs (g)(1) through (4) of this section, the Secretary shall notify the Archivist of the United States, who shall suspend pub-

lic access pending approval by the Director of ISOO. Any such decision made by the Director of ISOO may be appealed by the Secretary to the President through the National Security Advisor.

(h) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after DHS has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Presidential Records Act, 44 U.S.C. 2204(c)(1), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of Executive Order 13526, section 3.5. When it is necessary to classify or reclassify such information, it shall be done so on a document-by-document basis with the personal participation of and under the direction of the Secretary or Deputy Secretary.

§ 7.22 Classification pending review.

(a) Whenever persons who do not have original classification authority originate or develop information that they believe requires immediate classification and safeguarding, and no authorized original classifier is available, that person shall:

(1) Safeguard the information in a manner appropriate for the classification level they believe it to be;

(2) Apply the appropriate overall classification markings; and

(3) Within five working days, securely transmit the information to the organization that has appropriate subject matter interest and original classification authority.

(b) When it is not clear which component would be the appropriate original classifier, the information shall be sent to the Office of the Chief Security Officer, Administrative Security Division, to determine the appropriate organization.

(c) The applicable original classification authority shall decide within 30 days of receipt whether the information warrants classification pursuant to Executive Order 13526 and shall render such decision in writing.

§ 7.23 Emergency release of classified information.

(a) The DHS Undersecretary for Management has delegated to certain DHS